



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04L 9/32, G06F 1/00	A1	(11) International Publication Number: WO 98/07254 (43) International Publication Date: 19 February 1998 (19.02.98)
(21) International Application Number: PCT/GB97/02142 (22) International Filing Date: 8 August 1997 (08.08.97) (30) Priority Data: 9616737.4 9 August 1996 (09.08.96) GB (71) Applicant (for all designated States except US): UNIVERSITY COURT OF THE UNIVERSITY OF PAISLEY [GB/GB]; Paisley Campus, High Street, Paisley PA1 2BE (GB). (72) Inventors; and (75) Inventors/Applicants (for US only): CLARK, Douglas, Fraser [GB/GB]; University Court of the University of Paisley, Paisley Campus, High Street, Paisley PA1 2BE (GB). GALBRAITH, Farquhar, Spence [GB/GB]; University Court of the University of Paisley, Paisley Campus, High Street, Paisley PA1 2BE (GB). (74) Agent: MURGITROYD & COMPANY; 373 Scotland Street, Glasgow G5 8PT (GB).		(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG). Published <i>With international search report.</i>
(54) Title: DEVICE AND METHOD FOR SAFEGUARDING DATA TRANSFERRED BETWEEN MACHINES OPERATING WITHIN A NETWORK (57) Abstract Provision of a secure environment for transferring information in electronic format. Data is encoded before it is sent from a computer to a printer. The software encoding the data simultaneously generates a job specific code. This code must be employed to permit printing of the data.		

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LJ	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

1 **DEVICE AND METHOD FOR SAFEGUARDING DATA TRANSFERRED BETWEEN MACHINES**
2 **OPERATING WITHIN A NETWORK**

3 This invention relates to means for effecting security,
4 and in particular to means for safeguarding data
5 transferred between machines operating within a network
6 environment.

7
8 It is recognised that there are numerous situations
9 where although encryption of data prior to its saving
10 in a machine is inappropriate, it is nonetheless
11 desirable that the data is not easily accessible.
12 However when data is transferred between machines
13 within a network there is always the possibility that
14 the data could be picked up from the network link or
15 from a receiving machine.

16
17 A practical example would be the printing of a
18 confidential document. If the document is sent from a
19 computer to a printer both of which are networked,
20 there is the possibility that access to the document or
21 a portion thereof may be gained from the network link
22 or the printer server, or from a hard copy when the
23 report has printed.

24
25 According to the present invention there is provided

1 means to safeguard data transferred within a network
2 from data transmitting means to data receiving means
3 comprising:
4 data transmitting means;
5 encoding means associated with said data transmitting
6 means;
7 data receiving means;
8 decoding means associated with said data receiving
9 means; and
10 enabling means for the decoding means to allow the data
11 receiving means to utilize transferred data.

12
13 Preferably said encoding means includes software which
14 encodes data prior to its transfer from the data
15 transmitting means.

16
17 Additionally or alternatively said encoding means may
18 include hardware which encodes data prior to its
19 transfer from the data transmitting means.

20
21 Preferably the encoding means includes software which
22 generates the enabling means.

23
24 Additionally or alternatively the encoding means may
25 include hardware which generates the enabling means.

26
27 Preferably the enabling means is job specific.

28
29 Preferably the enabling means is an access code.

30
31 Preferably the decoding means is adapted for attachment
32 to the data receiving means. Alternatively the
33 decoding means may be remote from the data receiving
34 means. Alternatively the decoding means may be
35 integrated in the data receiving means.

36

1 Preferably the decoding means is a hardware device.

2

3 Preferably the decoding means includes means for input
4 of the enabling means.

5

6 Preferably the means for input of the enabling means is
7 a data entry device. More preferably the data entry
8 device is a keypad or a swipe.

9

10 Preferably said means to safeguard data denies access
11 to transferred data unless the decoding means is
12 enabled by the enabling means within a specified time
13 period from generation of the enabling means.

14

15 Preferably said means to safeguard data denies access
16 to transferred data if more than one unsuccessful
17 attempt is made to enable the decoding means.

18

19 Preferably the data transmitting means is a computer.

20

21 Preferably the data receiving means is a printer.

22

23 Alternatively the data receiving means may be a
24 computer.

25

26 Alternatively the data receiving means may be a
27 facsimile machine.

28

29 Further according to the present invention there is
30 provided a method of safeguarding data transferred
31 within a network from a computer to a printer,
32 comprising the steps of:
33 providing encoding means in the computer and decoding
34 means for the printer;
35 encoding the data and generating an access code in the
36 computer;

1 sending encoded data to the printer; and
2 applying the access code to the decoding means to
3 enable the decoding means and permit printing of the
4 data.

5
6 Preferably the method is applied to an existing
7 network.

8
9 Preferably the method is applied to the Internet.
10

11 Embodiments of the present invention will now be
12 described by way of example only.

13
14 A computer network comprises several client sharing
15 computers and one or several standard laser printer
16 facilities connected to a server. Data is generated
17 and saved on the computer prior to the generation of a
18 physical report.

19
20 To generate a report, data is sent to a printer either
21 directly or through a printer server. When a computer
22 user instructs the printing of particular data,
23 encoding means in the form of software encodes the
24 data. This software, which may be included in the
25 printer driver software, intercepts unencoded output
26 from a printer driver and encodes the information
27 before sending it to the printer server. In addition,
28 the software generates and displays enabling means for
29 each print job in the form of a job specific access
30 code. Thus the codes generated by the encoder software
31 form part of an encryption algorithm used in the coding
32 and decoding processes.

33
34 The data is sent over the network in the encoded form.
35 This ensures that any data picked up from the network
36 link, arriving at other than its designated address, or

1 stored on the printer server, is incomprehensible.
2
3 Decoding means controls the flow of data. The decoding
4 means incorporates a keypad and prevents decoding of
5 any data received by the decoding means unless the
6 correct code is entered in the keypad. A standard
7 laser printer has a port to accommodate memory and/or
8 font cartridges. Decoding means in the form of a
9 cartridge with the facility to register a code is
10 plugged into this port.
11
12 Alternatively discrete decoding means is inserted
13 between the computer or printer server and the printer.
14 This discrete decoding means may take the form of a box
15 including electronics, connectors and power switches.
16 Alternatively the electronics are incorporated on a
17 single chip and included in a printer cable - that is,
18 the decoding means is integrated in the printer cable.
19 The above options allow for the adaption of an existing
20 printer. The decoding means can be integrated in new
21 printers.
22
23 The decoding means comprises a microcontroller or
24 microprocessor or other programmable device which
25 controls the flow of data in both encrypted and non-
26 encrypted format between the computer and the printer.
27 The decoding means further includes ancillary
28 electronics. These ancillary electronics include
29 voltage stabilisation circuitry and buffering between
30 the decoding means and the computer and printer.
31 External features include an LCD display, a code input
32 device such as a keypad, connectors and power switches.
33 The processor controls the display output and the
34 keypad input, when it is necessary to enter the code.
35 When the correct code has been entered, the controller
36 also performs the decryption of the incoming data.

1 An intelligible output is obtainable only when the
2 correct code is entered in the decoding means. The
3 code is job specific and the decoding means can be
4 programmed to delete a print job, or store it
5 temporarily, or return it to the print server, unless
6 the correct job code is entered within a specified time
7 period from the print job being sent to the printer
8 from the print server, or if the wrong code is entered
9 more than once.

10

11 The advantages of this invention include its
12 simplicity. Its inclusion in an existing network
13 environment requires minimal adaptation of that
14 network. In essence all that is required is a code-
15 operated cartridge adapted for attachment to existing
16 printers or a stand alone box, and suitable software.

17

18 The software can be part of a printer driver or an
19 addition to the printer driver. When the printer
20 driver has coded the job for a specific printer, the
21 encryption driver intercepts this information before
22 sending it to the printer. The software algorithm is
23 platform and network independent, and runs on a variety
24 of platforms such as Windows™ or OS/2™, and networks
25 such as Novell™.

26

27 Since the information is sent to the printer in encoded
28 format it cannot be picked up from the network link in
29 intelligible form. Information stored on the printer
30 server is encoded and lost printouts are
31 incomprehensible. Thus confidential reports or the
32 like sent to a network printer from a computer or over
33 the Internet may be accessed only by the initiator of
34 the print job or someone authorised by them.

35

36 Access may similarly be denied to confidential

1 information sent from computer to computer or computer
2 to facsimile machine . The invention also facilitates
3 monitoring and/or restricting use of a printer.

4

5 Modifications and improvements may be made to the above
6 without departing from the scope of the invention.

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

1 CLAIMS

2

3 1. Means to safeguard data transferred within a
4 network from data transmitting means to data
5 receiving means comprising:
6 data transmitting means;
7 encoding means associated with said data
8 transmitting means;
9 data receiving means;
10 decoding means associated with said data receiving
11 means; and
12 enabling means for the decoding means to allow the
13 data receiving means to utilize transferred data.

14

15 2. Means to safeguard data as claimed in Claim 1
16 wherein the encoding means includes software which
17 encodes data prior to its transfer from the data
18 transmitting means.

19

20 3. Means to safeguard data as claimed in any
21 preceding claim wherein the encoding means
22 includes hardware which encodes data prior to its
23 transfer from the data transmitting means.

24

25 4. Means to safeguard data as claimed in any
26 preceding claim wherein the encoding means
27 includes software which generates the enabling
28 means.

29

30 5. Means to safeguard data as claimed in any
31 preceding claim wherein the encoding means
32 includes hardware which generates the enabling
33 means.

34

35 6. Means to safeguard data as claimed in any
36 preceding claim wherein the enabling means is job

- 1 specific.
2
3 7. Means to safeguard data as claimed in any
4 preceding claim wherein the enabling means is an
5 access code.
6
7 8. Means to safeguard data as claimed in any
8 preceding claim wherein the decoding means is
9 adapted for attachment to the data receiving
10 means.
11
12 9. Means to safeguard data as claimed in any
13 preceding claim wherein the decoding means is
14 remote from the data receiving means.
15
16 10. Means to safeguard data as claimed in any
17 preceding claim wherein the decoding means is
18 integrated in the data receiving means.
19
20 11. Means to safeguard data as claimed in any
21 preceding claim wherein the decoding means is a
22 hardware device.
23
24 12. Means to safeguard data as claimed in any
25 preceding claim wherein the decoding means
26 includes means for input of the enabling means.
27
28 13. Means to safeguard data as claimed in Claim 12
29 wherein the means for input of the enabling means
30 is a data entry device.
31
32 14. Means to safeguard data as claimed in Claim 13
33 wherein the data entry device is a keypad or a
34 swipe.
35
36 15. Means to safeguard data as claimed in any

- 1 preceding claim which denies access to transferred
2 data unless the decoding means is enabled by the
3 enabling means within a specified time period from
4 generation of the enabling means.
5
- 6 16. Means to safeguard data as claimed in any
7 preceding claim which denies access to transferred
8 data if more than one unsuccessful attempt is made
9 to enable the decoding means.
10
- 11 17. Means to safeguard data as claimed in any
12 preceding claim wherein the data transmitting
13 means is a computer.
14
- 15 18. Means to safeguard data as claimed in any
16 preceding claim wherein the data receiving
17 means is a printer.
18
- 19 19. Means to safeguard data as claimed in Claims 1 to
20 19 wherein the data receiving means is a computer.
21
- 22 20. Means to safeguard data as claimed in Claims 1 to
23 19 wherein the data receiving means is a facsimile
24 machine.
25
- 26 21. A method of safeguarding data transferred
27 within a network from a computer to a printer
28 comprising the steps of:
29 providing encoding means in the computer and
30 decoding means for the printer;
31 encoding the data and generating an access code in
32 the computer;
33 sending encoded data to the printer; and
34 applying the access code to the decoding means to
35 enable the decoding means and permit printing of
36 the data.

1 22. A method of safeguarding data as claimed in Claim
2 21 applied to an existing network.

3

4 23. A method of safeguarding data as claimed in Claim
5 21 applied to the Internet.

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

INTERNATIONAL SEARCH REPORT

International Application No

PCT/GB 97/02142

A. CLASSIFICATION OF SUBJECT MATTER

IPC 6 H04L9/32 G06F1/00

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 445 290 A (SECOM CO LTD) 11 September 1991 see page 2, line 3 - line 6 see page 4, line 9 - line 15 see page 5, line 35 - line 43 see page 5, line 47 - line 57 see page 6, line 31 - line 56	1,3,5,6, 8,11,15
A	---	20
X	EP 0 665 486 A (AT & T CORP) 2 August 1995 see column 1, line 34 - column 2, line 5 see column 3, line 6 - line 27 see column 4, line 13 - line 32 see column 5, line 12 - line 27 see column 6, line 35 - line 56 see column 7, line 43 - line 58 ---	1,4-6, 17-23
	-/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"d" document member of the same patent family

Date of the actual completion of the international search

18 November 1997

Date of mailing of the international search report

02/12/1997

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Larcinese, A

INTERNATIONAL SEARCH REPORT

International Application No

PCT/GB 97/02142

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>GB 2 188 758 A (BERTENSHAW PHILIP HALL; JONES JOHN; SEDGWICK ANTHONY) 7 October 1987 see page 1, left-hand column, line 15 - line 17 see page 1, left-hand column, line 41 - line 57 see page 1, right-hand column, line 82 - line 87 see page 1, right-hand column, line 96 - line 108 see page 1, right-hand column, line 116 - line 125 see page 2, right-hand column, line 90 - page 3, left-hand column, line 14 -----</p>	21-23

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter. Appl. Application No

PCT/GB 97/02142

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0445290 A	11-09-91	JP 2134940 A	23-05-90
		AT 149769 T	15-03-97
		CA 1337997 A	23-01-96
		DE 68927831 D	10-04-97
		DE 68927831 T	25-09-97
		WO 9006029 A	31-05-90
		KR 9400178 B	08-01-94
		US 5253293 A	12-10-93
EP 0665486 A	02-08-95	US 5509074 A	16-04-96
		CA 2137065 A	28-07-95
		JP 7239828 A	12-09-95
GB 2188758 A	07-10-87	NONE	